Fulfillment of HTTP Authentication Based on Alcatel OmniSwitch 9700

Hefu Liu
Center of Network and Education Technology, Huazhong Normal University, Wuhan, Hubei, China

Abstract. This paper provides a way of HTTP authentication On Alcatel OmniSwitch 9700. Authenticated VLANs control user access to network resources based on VLAN assignment and user authentication. The user can be authenticated through the switch via any standard Web browser software. Web browser client displays the username and password prompts. Then a way for HTML forms can be given to pass HTTP authentication data when it's submitted. A radius server will provide a database of user information that the switch checks whenever it tries to authenticate through the switch. Before or after authentication, the client can get an address from a Dhcp server.

1 Introduction

A VLAN (virtual local area network) is a collection of nodes that are grouped together in a single broadcast domain based on something other than physical location. A LAN in turn often connects to other LANs, and to the Internet or some other WAN. Authenticated VLANs control user access to network resources based on VLAN assignment and log-in process, and the process is sometimes called user authentication [4]. The type of security is device authentication, which is set up through the use of port-binding VLAN static port assignment.

On Alcatel OmniSwitch 9700, it can be realized that web browser clients authenticate through the switch via any standard Web browser software, which is based on AVLAN(Authenticated VLAN). Web browser client displays the username and password prompts. Then a way for HTML forms can be given to pass HTTP authentication data when it's submitted. So the implementation of HTTP authentication is simple and safe.

2 HTTP Authenticated Network Overview

An authenticated network involves several components as shown in this illustration.

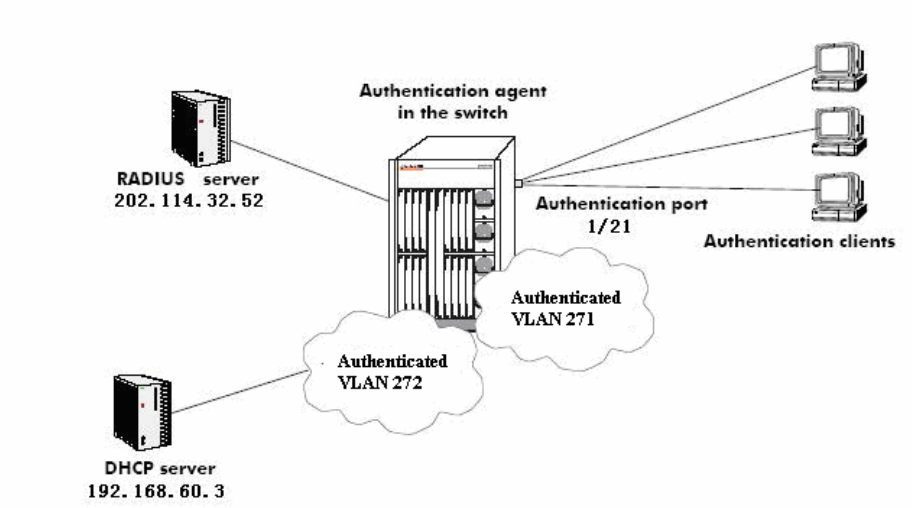

Fig. 1. HTTP Authenticated Network Components

This Fig.1 describes all of these components in detail. A brief overview of the components is given here:

RADIUS server—A RADIUS server must be configured in the network. The server contains a database of user information that the switch checks whenever a user tries to authenticate through the switch. The external server may also be used for authenticated switch access.

DHCP server—Web browser clients may get IP addresses via a DHCP server prior to authenticating or after authentication in order to move into a different VLAN. When multiple authenticated VLANs are configured, after the client authenticates the client must automatically issue a DHCP release/renew request in order to be moved into the correct VLAN.

Authentication port—At least one mobile port must be configured on the switch as an authentication port. This is the physical port through which authentication clients are attached to the switch.

Authentication clients—Authentication clients login through the switch to get access to authenticated VLANs.

Authenticated VLANs—Authenticated VLAN 272 is used to make the client get IP address before authentication, and after authentication ,the client will be moved into another VLAN 271.

Authentication agent in the switch—Authentication is enabled when the server(s) and the server authority mode is specified on the switch.

Configure a DNS name on the switch. A Domain Name Server (DNS) name may be configured so that Web browser clients may enter a URL on the browser command line instead of an authentication IP address. A Domain Name Server must be set up in the network for resolving the name to the authentication IP address. There may be multiple authentication IP addresses on the switch (if multiple authenticated VLANs are set up); however, there is only one authentication DNS path or host name. When the client enters the DNS path, the switch determines the IP authentication address based on the client's IP address, and the browser authentication page is displayed. A DNS name must be configured so that users may enter a URL rather than an IP address in the browser command line.

Typically the client address is provided by DHCP. DHCP also supplies DNS IP addresses to the client. The DHCP server must be configured with DNS addresses that correspond to the authenticated VLANs.

Normally, authentication clients cannot traffic in the default VLAN, so authentication clients do not belong to any VLAN when they connect to the switch. Even if DHCP relay is enabled, the DHCP discovery process cannot take place. To address this issue, a DHCP gateway address must be configured so that the DHCP relay "knows" which router port address to use for serving initial IP addresses.

When the client authenticates, the client is moved into the allowed VLAN based on VLAN information sent from an authentication server (single mode authority) or based on VLAN information configured directly on the switch (multiple mode authority).

After authentication a client may be moved into a VLAN in which the client's current IP address does not correspond. This will happen if the DHCP gateway address for assigning initial IP addresses is the router port of an authenticated VLAN to which the client does not belong. In this case, clients will automatically send DHCP release/renew requests to get an address in the authenticated VLAN to which they have access; DHCP relay must be enabled so that the request can be forwarded to the appropriate VLAN.

3 RADIUS Server Attributes

3.1 Introduction

RADIUS servers and RADIUS accounting servers are configured with particular attributes defined in RFC2138 and RFC 2139, respectively [4]. These attributes carry specific authentication, authorization, and configuration details about RADIUS requests to and replies from the server. This section describes the attributes and how to configure them on the server. The Standard RADIUS server attributes 1–39 and 60–63 are hardly supported by the Alcatel RADIUS client in the switch. However , attribute 26 is for vendor-specific information and is able to do these, and the standard attributes supported for RADIUS accounting servers of HTTP AUTHENTICATION.

3.2 Vendor-Specific Attributes for RADIUS

The Alcatel RADIUS client supports attribute 26, which includes a vendor ID and some additional subattributes called subtypes[3]. The vendor ID and the subtypes collectively are called Vendor Specific Attributes (VSAs). Alcatel, through partnering arrangements, has included these VSAs in some vendors'RADIUS server configurations. The attribute subtypes are defined in the server's dictionary file. If you are using single authority the first VSA subtype, **Alcatel-Auth-Group**, must be defined on the server for each authenticated VLAN.Alcatel's vendor ID is 800 (SMI Network Management Private Enterprise Code).
The following are necessary VSAs for RADIUS servers [1]:

Number	RADIUS VSA	Type	Description
1	Alcatel-Auth-Group	integer	The authenticated VLAN number. The only protocol associated with this attribute is Ethernet II. If other protocols are required, use the protocol attribute instead.
2	Alcatel-Slot-Port	string	Slot(s)/port(s) valid for the user.
3	Alcatel-Time-of-Day	string	The time of day valid for the user to authenticate.
4	Alcatel-Client-IP-Addr	address	The IP address used for Telnet only.
5	Alcatel-Group-Desc	string	Description of the authenticated VLAN.
6	Alcatel-Port-Desc	string	Description of the port.
7	Not Defined	Not Defined	Not Defined
8	Alcatel-Auth-Group-Protocol	string	The protocol associated with the VLAN. Must be configured for access to other protocols. Values include: IP_E2, IP_SNAP, IPX_E2, IPX_NOV,IPX_LLC, IPX_SNAP.
9	Alcatel-Asa-Access	string	Specifies that the user has access to the switch. The only valid value is all
10	Alcatel-End-User-Profile	string	Specifies the name of an end-user profile associated

3.3 Preparations For Web Browser Authentication Client

Web browser clients authenticate through the switch via any standard Web browser software (Netscape Navigator or Internet Explorer).

• **Make sure a standard browser is available on the client station**. No specialized client software is required.

• **Provide an IP address for the client**. Web browser clients require an address prior to thentication. The address may be statically assigned if the authentication network is set up in single authority mode with one authenticated VLAN. The

address may be assigned dynamically if a DHCP server is located in the network. DHCP is required in networks with multiple authenticated VLANs.

3.4 Fulfillment of HTTP Authentication

Before you perform HTTP authentication, you must have access to the Radius server and the Dhcp server form your switch.

First we must create two vlans such as vlan 271 and vlan 272,which are named radius and dhcprad.

Step 1 vlan 271 enable name radius

Step 2 vlan 272 enable name dhcprad

Step 3 ip interface radius address 202.114.39.1 mask 255.255.255.248 vlan 271

Step 4 ip interface dhcprad address 192.168.60.1 mask 255.255.255.0 vlan 272

Now ,Create and enable at least one mobile authenticated port. The port must be in VLAN 272.

Step 5 vlan 272 port default 1/21

Step 6 vlan port mobile 1/21

Step 7 vlan port 1/21 authenticate enable

After vlan authentication is set up the enable status, the switch will automatically create an authentication IP address based on this router port address (in this example, the address would be 192.168.60.253). The authentication address is configurable.

Step 8 vlan 271 authentication enable

Step 9 vlan 272 authentication enable

Set up a path to a DHCP server if users will be getting IP addresses from DHCP. The IP helper address is the IP address of the DHCP server; the AVLAN default DHCP address is the address of any router port configured on the VLAN. The DHCP server address is 192.168.60.3. The DHCP gateway address is 192.168.60.1.

Step 10 ip helper address 192.168.60.3

Step 11 aaa avlan default dhcp 192.168.60.1

Configure the switch to communicate with the authentication servers.

Step 12 aaa radius-server rad1 host 202.114.32.52 key testkey auth-port 1812 acct-port 1813

Enable authentication by specifying the authentication mode (single mode or multiple mode) and the server. Use the RADIUS or LDAP server name(s) configured in step 12.

Step 13 aaa authentication vlan single-mode rad1

At last, connect the PC you will be using to test to the appropriate slot and port configured above, bring up a web browser and enter the appropriate authentication address as the URL,https://192.168.60.253, and then enter the appropriate username and password when prompted.

4 Conclusion

The paper describes a simple HTTP Authentication mechanism that could be used in the B/S architecture.HTTP Authentication offers lots of advantages:

- It's simple to implement and no hassle to use, and clients love it.

- It carries no baggage unlike cookies.
- We can use HTTP Digest which is pretty secure and is easy to be understood.

So here we have discussed HTTP authentication method on Alcatel OmniSwitch 9700, there is no need for HTTP authentication to be shunned.

References

1. Alcatel Enterprise Data Training Course 9006-OmiSwitch Boot Camp
2. C. Rigney, A. Rubens, W. Simpson and S. Willens， "Remote Authentication Dial In User Service (RADIUS)"， *RFC 2138*， April 1997.
3. http://www.freeradius.org/rfc/
4. http://www.ietf.org/rfc/